Finite Fields and Their Applications **8,** 478–490 (2002)
doi:10.1006/ffta.2002.0355

The Number of Permutation Polynomials of a Given Degree Over a Finite Field

Pinaki Das

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802, USA
E-mail:das@math.psu.edu

Communicated by Daqing Wan

Received August 31, 2001; revised January 8, 2002; published online May 28, 2002

We relate the number of permutation polynomials in $\mathbf{F}_q[x]$ of degree $d \leq q-2$ to the solutions $(x_1, x_2, \ldots, x_q)$ of a system of linear equations over $\mathbf{F}_q$, with the added restriction that $x_i \neq 0$ and $x_i \neq x_j$ whenever $i \neq j$. Using this we find an expression for the number of permutation polynomials of degree $p-2$ in $\mathbf{F}_p[x]$ in terms of the permanent of a Vandermonde matrix whose entries are the primitive pth roots of unity. This leads to nontrivial bounds for the number of such permutation polynomials. We provide numerical examples to illustrate our method and indicate how our results can be generalised to polynomials of other degrees. © 2002 Elsevier Science (USA)

1. INTRODUCTION

Let $\mathbf{F}_q$ be the finite field of $q = p^r$ elements, where p is a prime and r is a positive integer. A polynomial f in $\mathbf{F}_q[x]$ is said to be a *permutation polynomial* if the induced map $\alpha \mapsto f(\alpha)$ from $\mathbf{F}_q$ to itself is bijective. For background material on permutation polynomials we refer to [3]. For algorithmic methods we refer to [6]. For a detailed survey of recent results we refer to [5]. The topic of this paper also appears as an open problem in [2].

In this paper, we first equate the number of permutation polynomials of a given degree to the number of solutions of a system of linear equations in $q-1$ variables over $\mathbf{F}_q$, with the added restriction that we only count those solutions $(x_1, x_2, \ldots, x_{q-1})$ for which $x_i \neq 0$ and $x_i \neq x_j$ whenever $i \neq j$ (Theorem 2.1).

1071-5797/02 $35.00

Next, we provide a formula for the number of permutation polynomials of degree $p-2$ over the field $\mathbf{F}_p$ in terms of the sum of the coefficients of pth powers of x in the expansion of the permanent of a Vandermonde matrix (Theorem 3.1). This makes it possible to write down a formula for the number of permutation polynomials of degree $p-2$ over the field $\mathbf{F}_p$ in terms of the permanent of a Vandermonde matrix whose entries are the pth roots of unity (Theorem 3.3). We indicate how to generalise our method to obtain expressions for the number of permutation polynomials of arbitrary degree $\leq p-2$, in terms of the sums of coefficients of certain terms which appear in the permanent of a Vandermonde matrix in several variables (Theorem 3.2).

We suggest some methods for evaluating the permanent of the Vandermonde matrix whose entries are the pth roots of unity. We use the Binet–Minc method to give a combinatorial formula for the number of permutation polynomials of degree $p-2$ over the field $\mathbf{F}_p$ (Theorem 4.2).

Finally, we give a nontrivial bound for the number of permutation polynomials of degree $p-2$ over $\mathbf{F}_p$ (Theorem 4.5). At several places in our exposition, we provide examples which illustrate our formulas and compare our results with numerical data in [3].

Additional remark. After the initial submission of this paper, a recent preprint [1] was brought to the notice of this author. In [1] the authors use exponential sums to find an asymptotic formula for the number of permutations for which the associated permutation polynomial has degree smaller than $q-2$. By contrast, we provide a simple formula for the number of permutation polynomials of degree $p-2$ in terms of the permanent of Vandermonde matrix whose entries are the pth roots of unity. Asymptotic bounds then follow from known results about upper bounds on the absolute value of the permanent of a complex matrix. In fact if $N_p(p-2)$ is the number of permutation polynomials $f \in \mathbf{F}_p[x]$ such that $f(0)=0$ and degree $(f)=p-2$ then it follows from the results of [1] that $|N_p(p-2)-\left(1-\frac{1}{p}\right)(p-1)!| \leq \sqrt{2e/\pi}\,p^{(p-2)/2}$. Our Theorem 4.5 shows that $|N_p(p-2)-\left(1-\frac{1}{p}\right)(p-1)!| \leq p^{(p-1)/2}$. Thus the bounds of [1] are asymptotically better only for a factor proportional to $\sqrt{p}$. We show in the example after Theorem 4.5 that $3,160,013 \leq N_{11}(9) \leq 3,437,805$. Using the results of [1] one could improve this to $3,235,031 \leq N_{11}(9) \leq 3,362,787$. On the other hand, both the estimates of [1] and Theorem 4.5 are far from being optimal.

Our method also provides a way to numerically compute the exact number of permutation polynomials of degree $p-2$. The authors of [1] note in their conclusion that although their ideas can be generalised to find asymptotic formulas for the number of permutation polynomials of degree

less than $q-2$, the exponential sums involved become significantly more complicated. We indicate how our results can be generalised in Theorem 3.2 and the example that follows.

2. PERMUTATION POLYNOMIALS AND SOLUTIONS OF A SYSTEM OF LINEAR EQUATIONS WITH RESTRICTIONS

It is easy to see that if f and g induce the same map on $\mathbf{F}_q$, then $f(x) \equiv g(x) \bmod (x^q - x)$. Furthermore, if $f(x)$ is a permutation polynomial and if a, b, c are elements of $\mathbf{F}_q$ with $a \neq 0$, then $af(x+b)+c$ is also a permutation polynomial over $\mathbf{F}_q$. Finally, if $d > 1$ is a divisor of $q-1$, then there is no permutation polynomial over $\mathbf{F}_q$ of degree d (see [3]). As a consequence, for our discussion it is enough to consider only polynomials f of degree $\leq q-2$ satisfying $f(0) = 0$.

Notation. For the rest of this paper we let $N_q(d)$ denote the number of permutation polynomials $f \in \mathbf{F}_q[x]$ such that $f(0) = 0$ and degree$(f) = d$, with $1 \leq d \leq q-2$.

Let $f(x) = \sum_{i=1}^{q-2} a_i x^i$ be a polynomial in $\mathbf{F}_q[x]$. Note that f has constant term zero and its degree is $\leq q-2$. Also let ω be a *primitive element* of $\mathbf{F}_q$. That is ω is a generator of the cyclic group $\mathbf{F}_q^{\times}$ (the group of units of $\mathbf{F}_q$). The image of f consists of the set of values $\{f(0) = 0, f(1), f(\omega), \ldots, f(\omega^{q-2})\}$.

Let W be the matrix defined by

$$W = (\omega^{(i-1)(j-1)})_{i,j=1,\ldots,q-1}.$$

Let $\mathbf{a}$ and $\mathbf{v}$ be the column vectors defined by

$$\mathbf{a} = (0 \ a_1 \ a_2 \ \cdots \ a_{q-2})^T \quad \text{and} \quad \mathbf{v} = (f(1) \ f(\omega) \ f(\omega^2) \ \cdots \ f(\omega^{q-2}))^T,$$

where T denotes the transpose of a matrix.

We call $\mathbf{a}$ the *coefficient vector* and $\mathbf{v}$ the *nonzero value vector* of the polynomial f. Note that for $0 \leq i \leq q-2$, the ith entry of a is the coefficient of x^i in the polynomial $f(x)$ and the ith entry of $\mathbf{v}$ is the value of $f(x)$ when $x = \omega^i$. It is easy to see that the coefficient vector and nonzero value vector of f are related by

$$W\mathbf{a} = \mathbf{v} \quad \text{and} \quad \mathbf{a} = W^{-1}\mathbf{v}.$$

Now if f is a permutation polynomial then the nonzero value vector $\mathbf{v}$ must be of the form $\mathbf{v} = P(1 \ \omega \ \omega^2 \ \cdots \ \omega^{q-2})^T$, where P is some permutation matrix which permutes the rows of $(1 \ \omega \ \omega^2 \ \cdots \ \omega^{q-2})^T$. Thus if f is a permutation polynomial we must have $W\mathbf{a} = P(1 \ \omega \ \omega^2 \ \cdots \ \omega^{q-2})^T$ and

$\mathbf{a} = W^{-1}P(1\ \omega\ \omega^2\ \cdots\ \omega^{q-2})^T$. Explicitly we have the following:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{q-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{q-2} & \omega^{2(q-2)} & \cdots & \omega^{(q-2)(q-2)} \end{pmatrix} \begin{pmatrix} 0 \\ a_1 \\ a_2 \\ \vdots \\ a_{q-2} \end{pmatrix} = P \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{q-2} \end{pmatrix} \tag{1}$$

and

$$\begin{pmatrix} 0 \\ a_1 \\ a_2 \\ \vdots \\ a_{q-2} \end{pmatrix} = (q-1)^{-1} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{q-2} & \omega^{2(q-2)} & \cdots & \omega^{(q-2)(q-2)} \\ 1 & \omega^{q-3} & \omega^{2(q-3)} & \cdots & \omega^{(q-2)(q-3)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega & \omega^2 & \cdots & \omega^{(q-2)} \end{pmatrix} P \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{q-2} \end{pmatrix} \tag{2}$$

We are now ready for the following theorem:

THEOREM 2.1. *Let E be the number of solutions in $\mathbf{F}_q$ of the system of equations*

$$\begin{aligned} x_1 + \omega^{q-d-1}x_2 + \omega^{2(q-d-1)}x_3 + \cdots + \omega^{(q-2)(q-d-1)}x_{q-1} &= 1, \\ x_1 + \omega^{q-d-2}x_2 + \omega^{2(q-d-2)}x_3 + \cdots + \omega^{(q-2)(q-d-2)}x_{q-1} &= 0, \\ &\vdots\ \vdots \\ x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{q-2}x_{q-1} &= 0, \end{aligned}$$

such that $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$.

Then $N_q(d) = (q-1)E$.

Proof. First, we observe that the number of solutions in $\mathbf{F}_q$ of

$$\begin{aligned} x_1 + \omega^{q-d-1}x_2 + \omega^{2(q-d-1)}x_3 + \cdots + \omega^{(q-2)(q-d-1)}x_{q-1} &\neq 0, \\ x_1 + \omega^{q-d-2}x_2 + \omega^{2(q-d-2)}x_3 + \cdots + \omega^{(q-2)(q-d-2)}x_{q-1} &= 0, \\ &\vdots\ \vdots \\ x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{q-2}x_{q-1} &= 0, \end{aligned}$$

such that $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$, is exactly $(q-1)E$. The proof of the theorem follows directly by comparing both sides of Eq. (2) with $a_1 = a_2 = \cdots = a_{d-1} = 0$, and $a_d \neq 0$. ∎

COROLLARY 2.2. *We have*

$$N_q(q-2) = (q-1)! - \#(x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{q-2} x_{q-1} = 0),$$

where # denotes the number of solutions in $\mathbf{F}_q$ *of the corresponding equation with the restriction that* $x_i \neq 0$ *and* $x_i \neq x_j$ *for* $i \neq j$.

In particular, the number $N_p(p-2)$ *of permutation polynomials* $f \in \mathbf{F}_p[x]$ *such that* $f(0) = 0$ *and* $\text{degree}(f) = p-2$, *is given by*

$$N_p(p-2) = (p-1)! - \#(x_1 + 2x_2 + 3x_3 + \cdots + (p-1)x_{p-1} \equiv 0 \bmod p),$$

with $x_i \neq 0$ *and* $x_i \neq x_j$ *for* $i \neq j$.

Proof. The proof follows from Theorem 2.1 above, once we observe that the sum of the two quantities $\#(x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{q-2} x_{q-1} \neq 0)$ and $\#(x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{q-2} x_{q-1} = 0)$ with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$ is exactly $(q-1)!$. ■

We also have

COROLLARY 2.3. *Let* $G_q(d)$ *be the number of solutions in* $\mathbf{F}_q$ *of the system of equations*

$$\begin{aligned}
x_1 + \omega^{q-d-1} x_2 + \omega^{2(q-d-1)} x_3 + \cdots + \omega^{(q-2)(q-d-1)} x_{q-1} &= 0,\\
x_1 + \omega^{q-d-2} x_2 + \omega^{2(q-d-2)} x_3 + \cdots + \omega^{(q-2)(q-d-2)} x_{q-1} &= 0,\\
&\vdots\\
x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{q-2} x_{q-1} &= 0,
\end{aligned}$$

such that $x_i \neq 0$ *and* $x_i \neq x_j$ *for* $i \neq j$.

Then

$$N_q(d) = (q-1)! - N_q(q-2) - N_q(q-3) - \cdots - N_q(d+1) - G_q(d).$$

Proof. Note that $G_q(q-2) = (q-1)! - N_q(q-2)$ and also that $N_q(q-3) + G_q(q-3) = G_q(q-2)$. The proof follows by induction. ■

3. GENERATING FUNCTION AND THE PERMANENT OF A VANDERMONDE MATRIX

We now proceed to find an exact formula for the number of permutation polynomials $f \in \mathbf{F}_p[x]$ such that $f(0) = 0$ and $\text{degree}(f) = p-2$. From Corollary 2.2 above, it suffices to find $\#(x_1 + 2x_2 + 3x_3 + \cdots + (p-1)x_{p-1} \equiv 0 \bmod p)$, with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$. We will find a

generating function for our problem in terms of the permanent of a Vandermonde matrix. We often use known results from the theory of permanents without proofs. For these and much more we refer to the text by Marcus and Minc [4]. First, we have the following definition:

DEFINITION. Let $A = (a_{ij})_{i,j=1,\ldots,n}$ be an $n \times n$ matrix. The *permanent* of A is defined by

$$\operatorname{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i\sigma(i)},$$

where S_n is the symmetric group of degree n and the sum is over all $n!$ permutations $\sigma \in S_n$.

We will use the following notation:

Notation. By $A = \text{Vandermonde}(z_1, z_2, \ldots, z_k)$ we will denote the $k \times k$ Vandermonde matrix whose (i,j)th term is given by $a_{ij} = z_j^{i-1}$, $i, j = 1, 2, \ldots, k$.

We want to count the number of solutions in $\mathbf{F}_p$ of $x_1 + 2x_2 + 3x_3 + \cdots + (p-1)x_{q-1} \equiv 0 \bmod p$, with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$. For this we consider a generating function. In our case the generating function is a polynomial $\Phi(x) \in \mathbf{Z}[x]$ such that for any integer n, the coefficient of x^n in $\Phi(x)$ gives the number of integer solutions of $x_1 + 2x_2 + 3x_3 + \cdots + (p-1)x_{p-1} = n$, with $1 \leq x_i \leq p-1$ and $x_i \neq x_j$ for $i \neq j$. Since we want all the x_i's to be distinct, the permanent is a natural choice for our generating function. In fact we have the following:

THEOREM 3.1. *Let* $A = \text{Vandermonde}(x, \ldots, x^{p-1})$. *In other words, let A be the matrix defined by* $A = (x^{(i-1)j})_{i,j=1,\ldots,p-1}$. *Also let* $\operatorname{per}(A) = \sum c_i x^i$. *Then*

$$\#(x_1 + 2x_2 + 3x_3 + \cdots + (p-1)x_{p-1} \equiv 0 \bmod p) = \sum_{i:\, p|i} c_i,$$

where # denotes the number of solutions in $\mathbf{F}_p$ *of the corresponding equation with the restriction that* $x_i \neq 0$ *and* $x_i \neq x_j$ *for* $i \neq j$ *and where the sum is over all those coefficients for which the exponent of x is divisible by p.*

Hence,

$$N_p(p-2) = (p-1)! - \sum_{i:\, p|i} c_i.$$

Proof. Consider the matrix B defined by

$$B = \begin{pmatrix} x & x^2 & x^3 & \cdots & x^{p-1} \\ x^2 & x^4 & x^8 & \cdots & x^{2(p-1)} \\ x^3 & x^6 & x^9 & \cdots & x^{3(p-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ x^{p-1} & x^{2(p-1)} & x^{3(p-1)} & \cdots & x^{(p-1)(p-1)} \end{pmatrix}.$$

Note that $\mathrm{per}(B) = x^{(p-1)/2}\,\mathrm{per}(A)$. It is clear that for any integer n, the coefficient of x^n in $\mathrm{per}(B)$ counts the number of solutions of $x_1 + 2x_2 + 3x_3 + \cdots + (p-1)x_{p-1} = n$, with $1 \le x_i \le p-1$ and $x_i \neq x_j$ for $i \neq j$. The proof of the theorem now follows once we observe that p divides the exponent $p(p-1)/2$ in $x^{p(p-1)/2}$. ■

EXAMPLE. Suppose we want to find the number of permutation polynomials of degree 5 in $\mathbf{F}_7[x]$. Let

$$A = \mathrm{Vandermonde}(x, x^2, \ldots, x^5) = (x^{(i-1)j})_{i,j=1,\ldots,6}.$$

Using Maple, we compute

$$\begin{aligned} \mathrm{Per}(A) = {} & x^{91} + 5x^{90} + 6x^{89} + 9x^{88} + 16x^{87} + 12x^{86} \\ & + 14x^{85} + 24x^{84} + 20x^{83} + 21x^{82} + 23x^{81} + 28x^{80} \\ & + 24x^{79} + 34x^{78} + 20x^{77} + 32x^{76} + 42x^{75} + 29x^{74} \\ & + 29x^{73} + 42x^{72} + 32x^{71} + 20x^{70} + 34x^{69} + 24x^{68} \\ & + 28x^{67} + 23x^{66} + 21x^{65} + 20x^{64} + 24x^{63} + 14x^{62} \\ & + 12x^{61} + 16x^{60} + 9x^{59} + 6x^{58} + 5x^{57} + x^{56}. \end{aligned}$$

The coefficients of x^n, $n = 56, 63, 70, 77, 84, 91$ are $1, 24, 20, 20, 24, 1$, respectively. Hence, the number of solutions of $x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 = 0$ in $\mathbf{F}_7$ with $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$ is $1 + 24 + 20 + 20 + 24 + 1 = 90$. Hence, the number of permutation polynomials of degree 5 and with constant term 0 in $\mathbf{F}_7[x]$ is $N_7(5) = 6! - 90 = 630$.

Lidl and Niederreiter [3, Table 7.1, p. 352] list normalised permutation polynomials. A polynomial f is in *normalised* form if f is monic, $f(0) = 0$ and when the degree n of f is not divisible by the characteristic p of $\mathbf{F}_q$, the coefficient of x^{n-1} is 0. It follows from the discussion in the beginning of Section 2 that it suffices to study normalised permutation polynomials. It is clear that to get the number of normalised permutation polynomials we simply divide the number of permutation polynomials with 0 constant term by $p(p-1)$. The list in [3] goes up to permutation polynomials of degree

≤ 5. We note that there are $\frac{630}{(7)(6)} = 15$ normalised permutation polynomials of degree 5 in $\mathbf{F}_7[x]$, which agrees with [3, Table 7.1, p. 352].

A similar calculation with Maple shows that there are 330,450 solutions of $x_1 + 2x_2 + \cdots + 10x_{10} = 0$ in $\mathbf{F}_{11}$ with $x_i \neq 0$ and $x_i \neq x_j$. Hence, the number of permutation polynomials of degree 9 and with constant term 0 in $\mathbf{F}_{11}[x]$ is $N_{11}(9) = 10! - 330,450 = 3,298,350$. Hence, the number of normalised permutation polynomials of degree 9 in $\mathbf{F}_{11}[x]$ is $\frac{3,298,350}{(11)(10)} = 29,985$.

It is possible to generalise our approach to systems of linear equations with restrictions as follows:

THEOREM 3.2. *Let*

$$A = \text{Vandermonde}(z_1 z_2 \cdots z_n, z_1^2 z_2^{2^2} \cdots z_n^{2^n}, \ldots, z_1^{p-1} z_2^{(p-1)^2} \cdots z_n^{(p-1)^n}),$$

where $1 \leq n \leq p-2$.

Also let $\text{per}(A) = \sum c_{i_1 i_2 \cdots i_n} z_1^{i_1} z_2^{i_2} \cdots z_n^{i_n}$. *Then the number of solutions in* $\mathbf{F}_p$ *of the system of equations*

$$\begin{aligned} x_1 + 2^n x_2 + 3^n x_3 + \cdots + (p-1)^n x_{p-1} &= 0, \\ x_1 + 2^{n-1} x_2 + 3^{n-1} x_3 + \cdots + (p-1)^{n-1} x_{p-1} &= 0, \\ &\vdots \\ x_1 + 2x_2 + 3x_3 + \cdots + (p-1) x_{p-1} &= 0, \end{aligned}$$

such that $x_i \neq 0$ *and* $x_i \neq x_j$ *for* $i \neq j$ *is equal to*

$$\sum_{p | i_1, \ldots, p | i_n} c_{i_1 i_2 \cdots i_n},$$

where the sum is over all those coefficients $c_{i_1 i_2 \cdots i_n}$ *for which* p *divides the exponent* i_k *of each* z_k.

Proof. The proof is similar to the proof of Theorem 3.1 above. ■

EXAMPLE. We can use Theorem 3.2 and Corollary 2.3 to compute the number of permutation polynomials in $\mathbf{F}_p[x]$ with zero constant term and of arbitrary degree d ($1 \leq d \leq p-2$). Using Maple to compute the permanent of Vandermonde $(z_1 z_2, z_1^2 z_2^4, \ldots, z_1^6 z_2^{36})$ we find that the sum of the coefficients of terms for which p divides the exponents of both z_1 and z_2 is 6. Hence (using the notation of Corollary 2.3) the number of permutation polynomials of degree 4 and constant term 0 in $\mathbf{F}_7[x]$ is given by $N_7(4) = (7-1)! - N_7(5) - G_7(4) = 6! - 630 - 6 = 84$. So the number of normalised permutation polynomials of degree 4 in $\mathbf{F}_7[x]$ is $\frac{84}{(7)(6)} = 2$, which agrees with [3, Table 7.1, p. 352].

We now derive a more useful formula for the number of permutation polynomials of degree $p-2$ in $\mathbf{F}_p[x]$. We have the following:

THEOREM 3.3. *Let $\zeta = e^{2\pi i/p}$ be a primitive pth root of unity and let $V = \text{Vandermonde}(\zeta, \zeta^2, \ldots, \zeta^{p-1})$, i.e. let $V = (\zeta^{(i-1)j})_{i,j=1,\ldots,p-1}$. Then*

$$\#(x_1 + 2x_2 + 3x_3 + \cdots + (p-1)x_{p-1} \equiv 0 \bmod p) = \frac{(p-1)! + (p-1)\,\text{per}(V)}{p},$$

where # denotes the number of solutions in $\mathbf{F}_p$ of the corresponding equation with the restriction that $x_i \neq 0$ and $x_i \neq x_j$ for $i \neq j$.

Hence

$$N_p(p-2) = \left(1 - \frac{1}{p}\right)((p-1)! - \text{per}(V)).$$

Proof. As in Theorem 3.1 let $A = \text{Vandermonde}(x, x^2, \ldots, x^{p-1})$, i.e. let $A = (x^{(i-1)j})_{i,j=1,\ldots,p-1}$. Let us write $f(x) = \text{per}(A) = \sum c_i x^i$. Clearly,

$$\sum_{k=0}^{p-1} f(\zeta^k) = p \sum_{i:\, p|i} c_i.$$

Also when $k = 0$, $f(1) = (p-1)!$, since it is the permanent of a $(p-1) \times (p-1)$ matrix with each entry $= 1$. Finally, for any $1 \leq k \leq p-1$ we have $f(\zeta^k) = f(\zeta)$, since substituting $x = \zeta^k$, $(1 \leq k \leq p-1)$, in the matrix A simply permutes the rows of A. The proof of the first statement now follows from Theorem 3.1 since $\#(x_1 + 2x_2 + 3x_3 + \cdots + (p-1)x_{p-1} \equiv 0 \bmod p) = \sum_{i:\, p|i} c_i$.

The final statement of the theorem is immediate from Corollary 2.2. ∎

4. EVALUATING PER (V) AND A BOUND FOR THE NUMBER OF PERMUTATION POLYNOMIALS

We will use the Binet–Minc method to derive another expression for the number of permutation polynomials of degree $p-2$. First, we need to fix some notations. Let $[n] = \{1, 2, \ldots, n\}$. A (set) *partition* π of $[n]$ is collection of disjoint subsets $\pi_1, \pi_2, \ldots, \pi_t$ of $[n]$ such that $\pi_1 \cup \cdots \cup \pi_t = [n]$. Let $d_i = |\pi_i|$, $1 \leq i \leq t$. The set of all partitions of $[n]$ is denoted by $\Pi([n])$. Finally, we recall that the Hadamard (entrywise) product of a finite number of $m \times n$ matrices is the $m \times n$ matrix whose ijth term is the product of the ijth terms of each individual matrix. In the following, we need to consider the Hadamard product of certain row vectors of a given matrix. We are

ready for the following theorem which describes the Binet–Minc method for computing the permanent of a matrix.

THEOREM 4.1. (Binet–Minc). *Let* $A = (a_{ij})$ *be an* $n \times n$ *matrix. Then* (*with notation as above*),

$$\operatorname{per}(A) = \sum_{\pi \in \Pi([n])} (-1)^{n-t}(d_1 - 1)! \cdots (d_t - 1)!\, r_{\pi_1} \cdots r_{\pi_t},$$

where r_{π_j} *is the sum of the entries in the Hadamard* (*entrywise*) *product of the rows of A indexed by* π_j.

The above theorem gives us a combinatorial expression for the number of permutation polynomials of degree $p-2$ as follows:

THEOREM 4.2. *Let* $V = \text{Vandermonde}(\zeta, \zeta^2, \ldots, \zeta^{p-1})$, *where* ζ *is a primitive* $(p-1)$*th root of unity. Then* (*with notation as above*),

$$\operatorname{per}(V) = \sum_{\pi \in \Pi([p-1])} (-1)^{p-1-t}(d_1 - 1)! \cdots (d_t - 1)!\, C(\pi_1) \cdots C(\pi_t),$$

where $C(\pi_j) = p-1$ *if* p *divides the sum of the elements in the block* π_j *and* $C(\pi_j) = -1$ *otherwise.*

Hence

$$N_p(p-2) = \left(1 - \frac{1}{p}\right) \times \left((p-1)! - \sum_{\pi \in \Pi([p-1])} (-1)^{p-1-t}(d_1 - 1)! \cdots (d_t - 1)! C(\pi_1) \cdots C(\pi_t)\right).$$

Proof. If p divides the sum of the elements in the block π_j then the Hadamard (entrywise) product of the rows of A indexed by π_j consists of a row of $p-1$ ones. Hence with notation as in Theorem 4.1, we have $r_{\pi_j} = p-1$ in this case. On the other hand if p does not divide the sum of the elements in the block π_j then the Hadamard (entrywise) product of the rows of A indexed by π_j consists of powers of a primitive pth root of unity whose sum is -1. Hence $r_{\pi_j} = -1$. The proof of the first statement is now clear from Theorem 4.1.

The second statement follows directly from Theorem 3.3. ■

Remark. We point out that there are algorithms such as Ryser's method, to compute permanents. Thus our approach provides a way to numerically compute $N_p(p-2)$. We do not discuss Ryser's method here, since it is described in some detail in [4]. Instead we use the permanent

to bound the number of permutation polynomials of degree $p-2$ as follows:

Let A be a complex square matrix and let A^* be the conjugate transpose of A. The *singular values* of the matrix A are defined to be the square roots of the eigenvalues of the matrix AA^*. We have the following result of Marcus and Minc on the lower bound of the permanent of a complex matrix.

THEOREM 4.3. *Let A be a complex $n \times n$ matrix and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the singular values of A. Then*

$$|\mathrm{per}(A)|^2 \leq \frac{1}{n} \sum_{i}^{n} \alpha_i^{2n}.$$

Proof. For a proof of the theorem we refer to [4]. ■

We can use the above result to find a bound for $\mathrm{per}(V)$, where V is the Vandermonde matrix in Theorem 4.2. We have the following:

THEOREM 4.4. *Let $V = \mathrm{Vandermonde}(\zeta, \zeta^2, \ldots, \zeta^{p-1})$, where ζ is a primitive pth root of unity. Then*

$$|\mathrm{per}(V)| \leq \sqrt{\frac{1 + (p-2)p^{p-1}}{p-1}}.$$

Proof. A direct computation shows that

$$VV^* = \begin{pmatrix} p-1 & -1 & -1 & \ldots & -1 \\ -1 & p-1 & -1 & \ldots & -1 \\ \vdots & \vdots & \vdots & & \vdots \\ -1 & -1 & -1 & \ldots & p-1 \end{pmatrix}.$$

It is an easy exercise to show that the characteristic polynomial $\det(xI - VV^*) = (x-1)(x-p)^{p-2}$. So VV^* has eigenvalues 1 and p (with multiplicities 1 and $p-2$, respectively). The proof now follows from Theorem 4.3. ■

THEOREM 4.5. *We have the following bounds*:

$$N_p(p-2) \geq \left(1 - \frac{1}{p}\right)\left((p-1)! - \sqrt{\frac{1 + (p-2)p^{p-1}}{p-1}}\right).$$

Also,

$$N_p(p-2) \leq \left(1-\frac{1}{p}\right)\left((p-1)!+\sqrt{\frac{1+(p-2)p^{p-1}}{p-1}}\right).$$

Proof. The bounds follow directly from Theorem 4.4 above and Theorem 3.3. ■

EXAMPLE. For example for $p = 11$, Theorem 4.5 gives the bounds

$$3,160,013 \leq N_{11}(9) \leq 3,437,805,$$

for the number of permutation polynomials of degree 9 and with constant term 0 in $\mathbf{F}_{11}[x]$. We saw in an earlier example (after Theorem 3.1) that the exact number is $N_{11}(9) = 3,298,350$.

5. CONCLUSION

In this paper we have mostly focussed our attention on permutation polynomials of degree $p-2$ over the field of p elements. We have indicated how to proceed in the general case in Theorems 2.1, 3.2 and Corollary 2.3. It should be possible to generalise our results to formulas and bounds for permutation polynomials of arbitrary degree over fields of prime power elements. This will be the subject of a separate paper. Another problem worth exploring is the problem of finding better bounds for the number of permutation polynomials of degree $p-2$. One possible approach is to find a better bound for the permanent of the Vandermonde matrix of Theorem 4.2.

ACKNOWLEDGMENTS

I thank Greg Anderson, Gary Mullen and Daqing Wan for their helpful comments after reading the first draft of this paper. I also thank the referee for helpful comments and suggestions.

REFERENCES

1. S. Konyagin and F. Pappalardi, Enumerating permutation polynomials over finite fields by degree, preprint, 2001.
2. R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? *Amer. Math. Monthly* **95** (1988), 243–246.

3. R. Lidl and H. Niederreiter, ''Finite Fields,'' Encyclopedia of Mathematics and its Applications, Vol. 20, Cambridge University Press, Cambridge, UK, 1997.
4. M. Marcus and H. Minc, ''Permanents,'' Encyclopedia of Mathematics and its Applications, Vol. 6, Addison–Wesley, Reading, MA, 1978.
5. G. L. Mullen, Permutation polynomials over finite fields, ''Finite Fields, Coding Theory, and Advances in Communications and Computing,'' pp. 131–151, Marcel Dekker, New York, 1993.
6. I. E. Shparlinski, ''Finite Fields: Theory and Computation,'' Mathematics and its Applications, Vol. 477, Kluwer Academic Publishers, Dordrecht, 1999.